Spyware: *dalla parte dell'attaccante*

Matteo G.P. Flora

29 Gennaio 2005

Matteo G.P. Flora

- Direttore IT
  - Al Village S.r.l.
- Titolare
  - LK Project Security
- Presidente Provinciale
  - A.I.P. (Associazione Informatici Professionisti)
- Perito e Consulente Tecnico
  - Tribunale della Procura della Repubblica di Milano
  - Nucleo Regionale GdF – Gruppo Repressione Frodi informatiche
  - Nucleo Provinciale GdF – Servizi Speciali

Spyware: una definizione

Definizione formale ed esempi

Cos'è uno Spyware

- Definizione

  "Si definisce **spyware** un tipo di software che raccoglie informazioni riguardanti un utente senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, oppure modifica le funzionalità del sistema in modo non trasparente all'utente a fini economici."

  (Fonte: Wikipedia.it)

Mascheramento

- Installazione

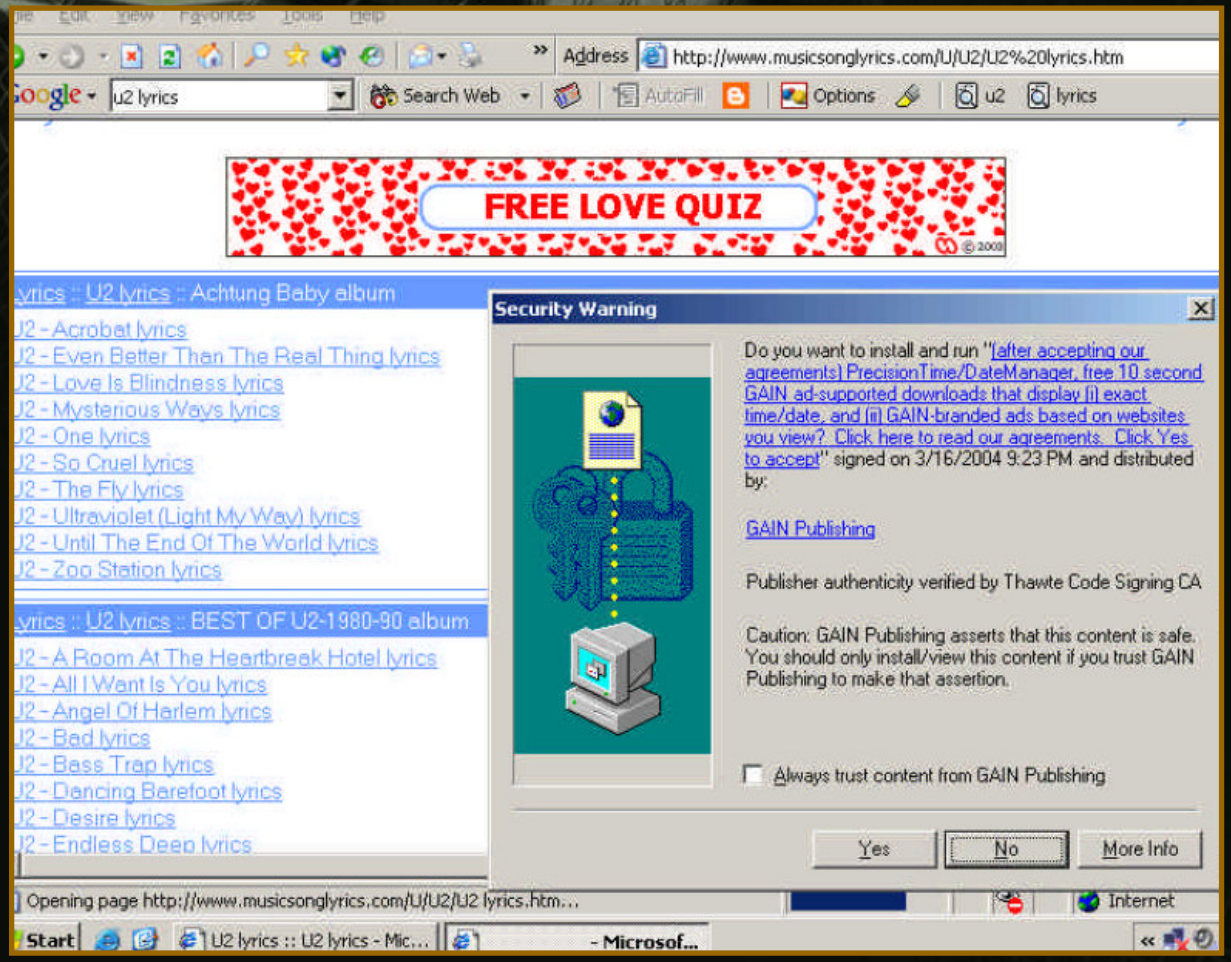
  Spesso non è possibile riconoscere l'installazione o essa viene fatta senza l'autorizzazione dell'utente.

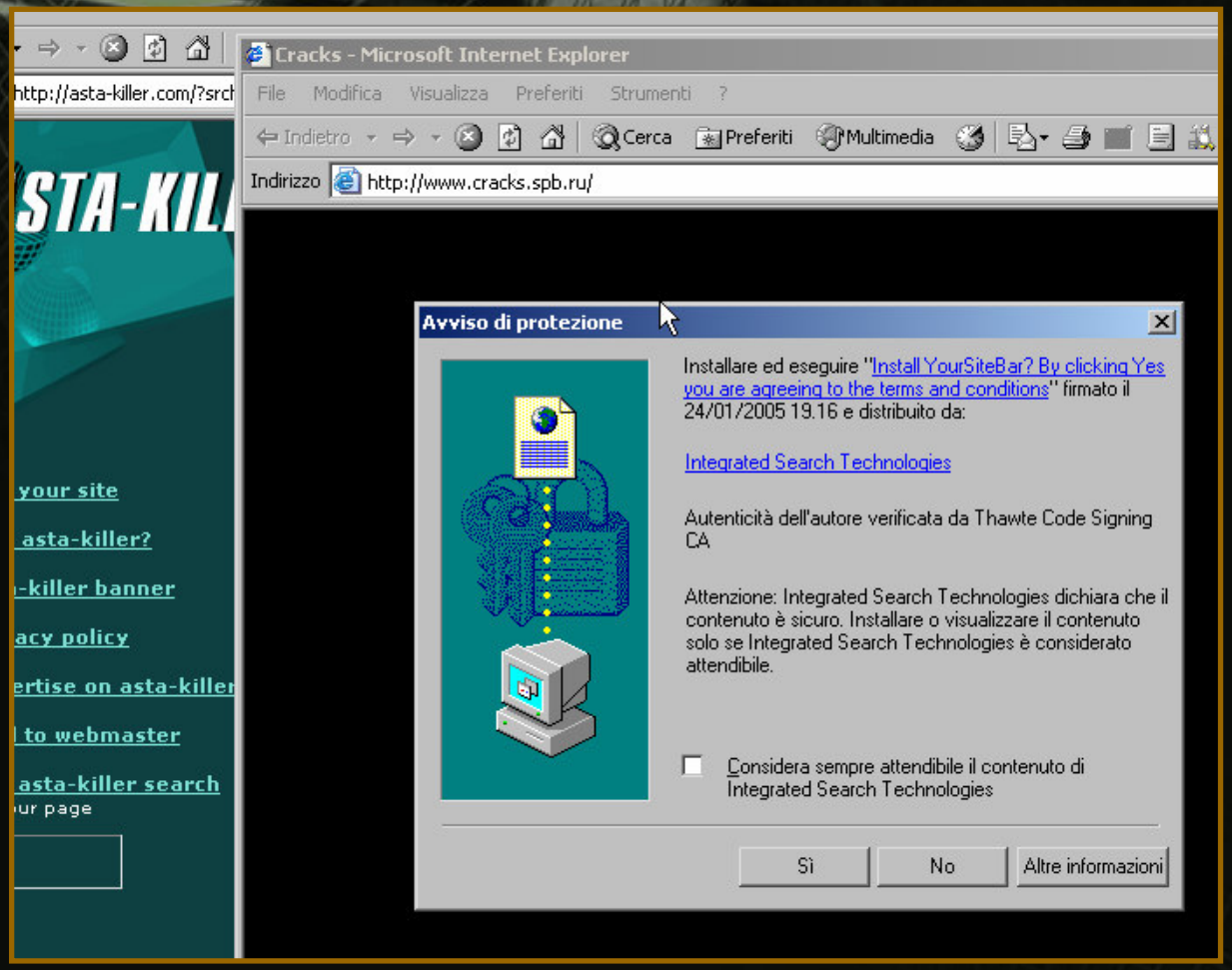
- Disclaimer fraudolenti

  Le condizioni di utilizzo proposte non sono chiare e/o sono incomprensibili.
  Claria ha un contratto di licenza della lunghezza della Divina Commedia (1M).

- Violazione delle Condizioni Contrattuali

  Inoltre spesso sono infrante apertamente dallo stesso produttore, parzialmente coperte da sofismi legali e/o cavilli burocratici.


Address http://www.musicsonglyrics.com/U/U2/U2%20lyrics.htm
u2 lyrics
Search Web
Options
u2
lyrics
FREE LOVE QUIZ
Achtung Baby album
U2 - Acrobat lyrics
U2 - Even Better Than The Real Thing lyrics
U2 - Love Is Blindness lyrics
U2 - Mysterious Ways lyrics
U2 - One lyrics
U2 - So Cruel lyrics
U2 - The Fly lyrics
U2 - Ultraviolet (Light My Way) lyrics
U2 - Until The End Of The World lyrics
U2 - Zoo Station lyrics
BEST OF U2-1980-90 album
U2 - A Room At The Heartbreak Hotel lyrics
U2 - All I Want Is You lyrics
U2 - Angel Of Harlem lyrics
U2 - Bad lyrics
U2 - Bass Trap lyrics
U2 - Dancing Barefoot lyrics
U2 - Desire lyrics
U2 - Endless Deep lyrics
Security Warning
Do you want to install and run "[after accepting our agreements] PrecisionTime/DateManager, free 10 second GAIN ad-supported downloads that display (i) exact time/date, and (ii) GAIN-branded ads based on websites you view? Click here to read our agreements. Click Yes to accept" signed on 3/16/2004 9:23 PM and distributed by:
GAIN Publishing
Publisher authenticity verified by Thawte Code Signing CA
Caution: GAIN Publishing asserts that this content is safe. You should only install/view this content if you trust GAIN Publishing to make that assertion.
Always trust content from GAIN Publishing
Yes
No
More Info
Opening page http://www.musicsonglyrics.com/U/U2/U2 lyrics.htm...
Internet
Start
U2 lyrics :: U2 lyrics - Mic...
- Microsof...


Cracks - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti Multimedia
Indirizzo http://www.cracks.spb.ru/
http://asta-killer.com/?srch
STA-KILL
your site
asta-killer?
-killer banner
acy policy
ertise on asta-killer
to webmaster
asta-killer search
ur page
Avviso di protezione
Installare ed eseguire "Install YourSiteBar? By clicking Yes you are agreeing to the terms and conditions" firmato il 24/01/2005 19.16 e distribuito da:
Integrated Search Technologies
Autenticità dell'autore verificata da Thawte Code Signing CA
Attenzione: Integrated Search Technologies dichiara che il contenuto è sicuro. Installare o visualizzare il contenuto solo se Integrated Search Technologies è considerato attendibile.
Considera sempre attendibile il contenuto di Integrated Search Technologies
Sì
No
Altre informazioni

Statistiche

- Diffusione

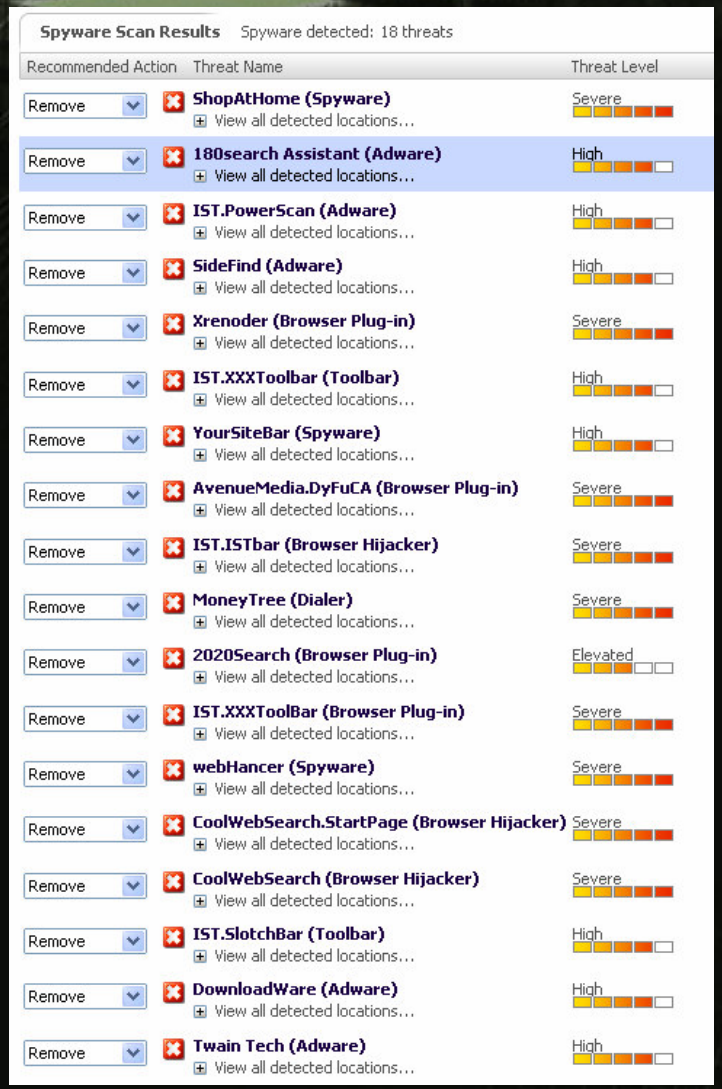
  Attualmente (Luglio 2004) le macchine infetta da uno dei 5 spyware più famosi sono circa 64.000.000

- Distribuzione

  Un computer connesso ad Internet che utilizza Internet Explorer per la navigazione "non a rischio" è normalmente affetto da ventiquattro (24) spyware entro il primo mese di vita.

- Soglia di pericolo

  L'utilizzo di Internet Explorer per la navigazione "particolare" comporta una infezione media di circa centottacentottanta (180) spyware entro i primi 6 mesi dall'installazione.


Spyware Scan Results
Spyware detected: 18 threats
Recommended Action
Threat Name
Threat Level
Remove
ShopAtHome (Spyware)
View all detected locations...
Severe
Remove
180search Assistant (Adware)
View all detected locations...
High
Remove
IST.PowerScan (Adware)
View all detected locations...
High
Remove
SideFind (Adware)
View all detected locations...
High
Remove
Xrenoder (Browser Plug-in)
View all detected locations...
Severe
Remove
IST.XXXToolbar (Toolbar)
View all detected locations...
High
Remove
YourSiteBar (Spyware)
View all detected locations...
High
Remove
AvenueMedia.DyFuCA (Browser Plug-in)
View all detected locations...
Severe
Remove
IST.ISTbar (Browser Hijacker)
View all detected locations...
Severe
Remove
MoneyTree (Dialer)
View all detected locations...
Severe
Remove
2020Search (Browser Plug-in)
View all detected locations...
Elevated
Remove
IST.XXXToolBar (Browser Plug-in)
View all detected locations...
Severe
Remove
webHancer (Spyware)
View all detected locations...
Severe
Remove
CoolWebSearch.StartPage (Browser Hijacker)
View all detected locations...
Severe
Remove
CoolWebSearch (Browser Hijacker)
View all detected locations...
Severe
Remove
IST.SlotchBar (Toolbar)
View all detected locations...
High
Remove
DownloadWare (Adware)
View all detected locations...
High
Remove
Twain Tech (Adware)
View all detected locations...
High

Danni

- Fuga di notizie
  - Lo spyware costituisce una seria lesione alla Privacy personale
- Stress
  - Una macchina affetta da spyware presenta all'utente circa 90 schermate pubblicitarie/giorno, alcune delle quali contenenti testi o immagini osceni.
- Utilizzo illecito del PC
  - Spesso i programmi di spyware utilizzano le risorse del computer a fini di calcoli distribuiti e a fine di spam verso altre macchine, oltre che per la installazione di altro software.
- Diminuzione di prestazioni
  - Una macchina infettata con spyware rallenta la propria velocità di navigazione sino al 70% e le sue prestazioni quando connessa in rete sino al 98%

Spyware in Azione

Un investimento conveniente

Gamma di servizi

- Pageviews di banner
  - Presentazione di banner pubblicitari
- Sostituzione di Banner concorrenti
  - Alterazione di siti e/o avvisi esistenti per la sostituzione di banner pubblicitari con case concorrenti
- Acquisizione dati di navigazione
  - Dati di marketing statistico e profiling degli utenti
- Commission theft
  - Alterazione dei sistemi di commissioni online
- Installazione Software non autorizzati
  - Alterazione della macchina a fini legali o meno.

SpyBanner: investimento vincente

- Funzione storica

  La presentazione di banner pubblicitari e/o la sostituzione di Home Page sono uno dei cardini storici dello spyware.

- Bassissimi costi

  Al contrario di molti network la presentazione di un banner nel circuito di Claria/WhenU ha costi di $.0,002 contro $.0.05 dei concorrenti.
  In campo preatico significa 1/20 dell'investimento.

- Aggiramento sistemi anti-banner

  I banner erogati dagli spyware non sono bloccabili, al contrario di quelli somministrati da siti web

SpyBanner: investimento vincente

- Profiling d'eccezione

  Lo spyware mantiene la storia di navigazione dell'utente, ed è in grado di proporre banner in sintonia.

- Controllo della navigazione

  E' possibile erogare un banner in occasione della visita di precisi siti web e/o precise parole contenute nella pagina visitata.

- Integrazione con il sistema operativo

  L'alta integrazione consente di controllare anche applicazioni non propriamente inerenti la navigazione web (messenger, work, outlook…)

Mascheramento e sostituzione

- La scalata del banner

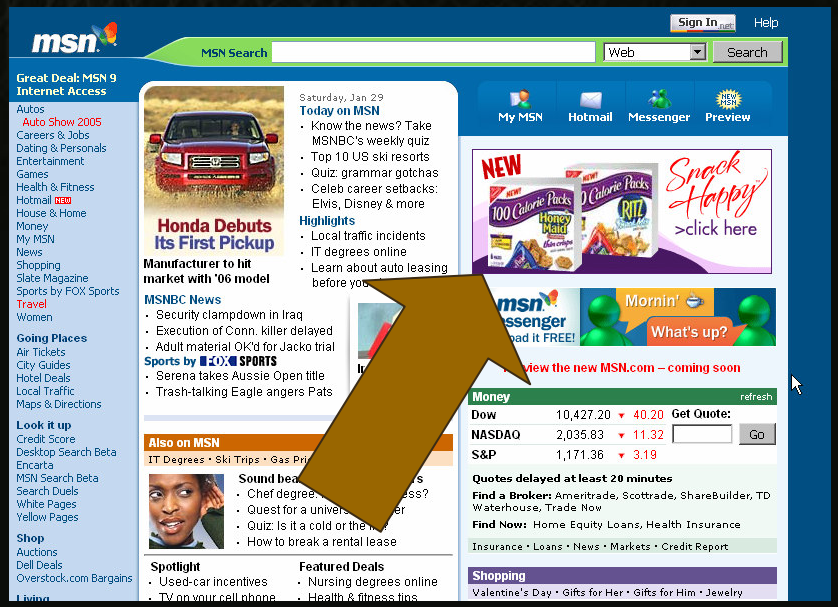
  La pubblicazione dei banner in network internazionali nelle posizioni di vertice è un costo esorbitante, in linae con i massimi quitidiani, accessibile solamente a potenti Corporate.

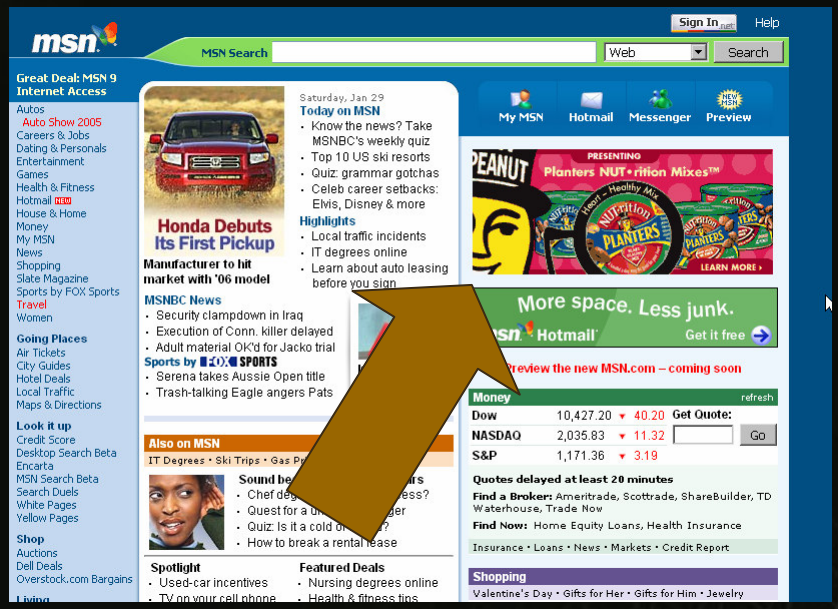
- La via economica

  E' molto più semplice permettere allo spyware di sostituire banner legittimi con i propri. In campo pratico significa un costo che può essere ridotto sino a 1/150 dell'investimento.

- Siti Affetti

  Tra gli altri ricordiamo: MSN, Yahoo, Amazon, Google, Lycos, Altavista, A9, CNN, The New York Times, CBS, NBC, Barnes&Nobles.


msn
Sign In
Help
MSN Search
Web
Search
Great Deal: MSN 9 Internet Access
Autos
Auto Show 2005
Careers & Jobs
Dating & Personals
Entertainment
Games
Health & Fitness
Hotmail
House & Home
Money
My MSN
News
Shopping
Slate Magazine
Sports by FOX Sports
Travel
Women
Going Places
Air Tickets
City Guides
Hotel Deals
Local Traffic
Maps & Directions
Look it up
Credit Score
Desktop Search Beta
Encarta
MSN Search Beta
Search Duels
White Pages
Yellow Pages
Shop
Auctions
Dell Deals
Overstock.com Bargains
Saturday, Jan 29
Today on MSN
Know the news? Take MSNBC's weekly quiz
Top 10 US ski resorts
Quiz: grammar gotchas
Celeb career setbacks: Elvis, Disney & more
Highlights
Local traffic incidents
IT degrees online
Learn about auto leasing
Honda Debuts Its First Pickup
Manufacturer to hit market with '06 model
MSNBC News
Security clampdown in Iraq
Execution of Conn. killer delayed
Adult material OK'd for Jacko trial
Sports by FOX SPORTS
Serena takes Aussie Open title
Trash-talking Eagle angers Pats
My MSN
Hotmail
Messenger
Preview
NEW
100 Calorie Packs
Honey Maid
RITZ
Snack Happy
>click here
Mornin'
What's up?
Money
refresh
Dow 10,427.20 40.20 Get Quote:
NASDAQ 2,035.83 11.32
S&P 1,171.36 3.19
Go
Quotes delayed at least 20 minutes
Find a Broker: Ameritrade, Scottrade, ShareBuilder, TD Waterhouse, Trade Now
Find Now: Home Equity Loans, Health Insurance
Insurance • Loans • News • Markets • Credit Report
Also on MSN
Spotlight
Used-car incentives
Featured Deals
Nursing degrees online
Shopping
Valentine's Day • Gifts for Her • Gifts for Him • Jewelry


msn
Sign In
Help
MSN Search
Web
Search
Great Deal: MSN 9 Internet Access
Autos
Auto Show 2005
Careers & Jobs
Dating & Personals
Entertainment
Games
Health & Fitness
Hotmail
House & Home
Money
My MSN
News
Shopping
Slate Magazine
Sports by FOX Sports
Travel
Women
Going Places
Air Tickets
City Guides
Hotel Deals
Local Traffic
Maps & Directions
Look it up
Credit Score
Desktop Search Beta
Encarta
MSN Search Beta
Search Duels
White Pages
Yellow Pages
Shop
Auctions
Dell Deals
Overstock.com Bargains
Saturday, Jan 29
Today on MSN
Know the news? Take MSNBC's weekly quiz
Top 10 US ski resorts
Quiz: grammar gotchas
Celeb career setbacks: Elvis, Disney & more
Highlights
Local traffic incidents
IT degrees online
Learn about auto leasing
Honda Debuts Its First Pickup
Manufacturer to hit market with '06 model
MSNBC News
Security clampdown in Iraq
Execution of Conn. killer delayed
Adult material OK'd for Jacko trial
Sports by FOX SPORTS
Serena takes Aussie Open title
Trash-talking Eagle angers Pats
My MSN
Hotmail
Messenger
Preview
PRESENTING
Planters NUT•rition Mixes™
LEARN MORE
More space. Less junk.
Hotmail
Get it free
Money
refresh
Dow 10,427.20 40.20 Get Quote:
NASDAQ 2,035.83 11.32
S&P 1,171.36 3.19
Go
Quotes delayed at least 20 minutes
Find a Broker: Ameritrade, Scottrade, ShareBuilder, TD Waterhouse, Trade Now
Find Now: Home Equity Loans, Health Insurance
Insurance • Loans • News • Markets • Credit Report
Also on MSN
Spotlight
Used-car incentives
Featured Deals
Nursing degrees online
Shopping
Valentine's Day • Gifts for Her • Gifts for Him • Jewelry

Mascheramento e sostituzione

- Sostituire un sito web

  Ancora più efficace è sostituire il sito web navigato dall'utente con il proprio, competitor diretto.

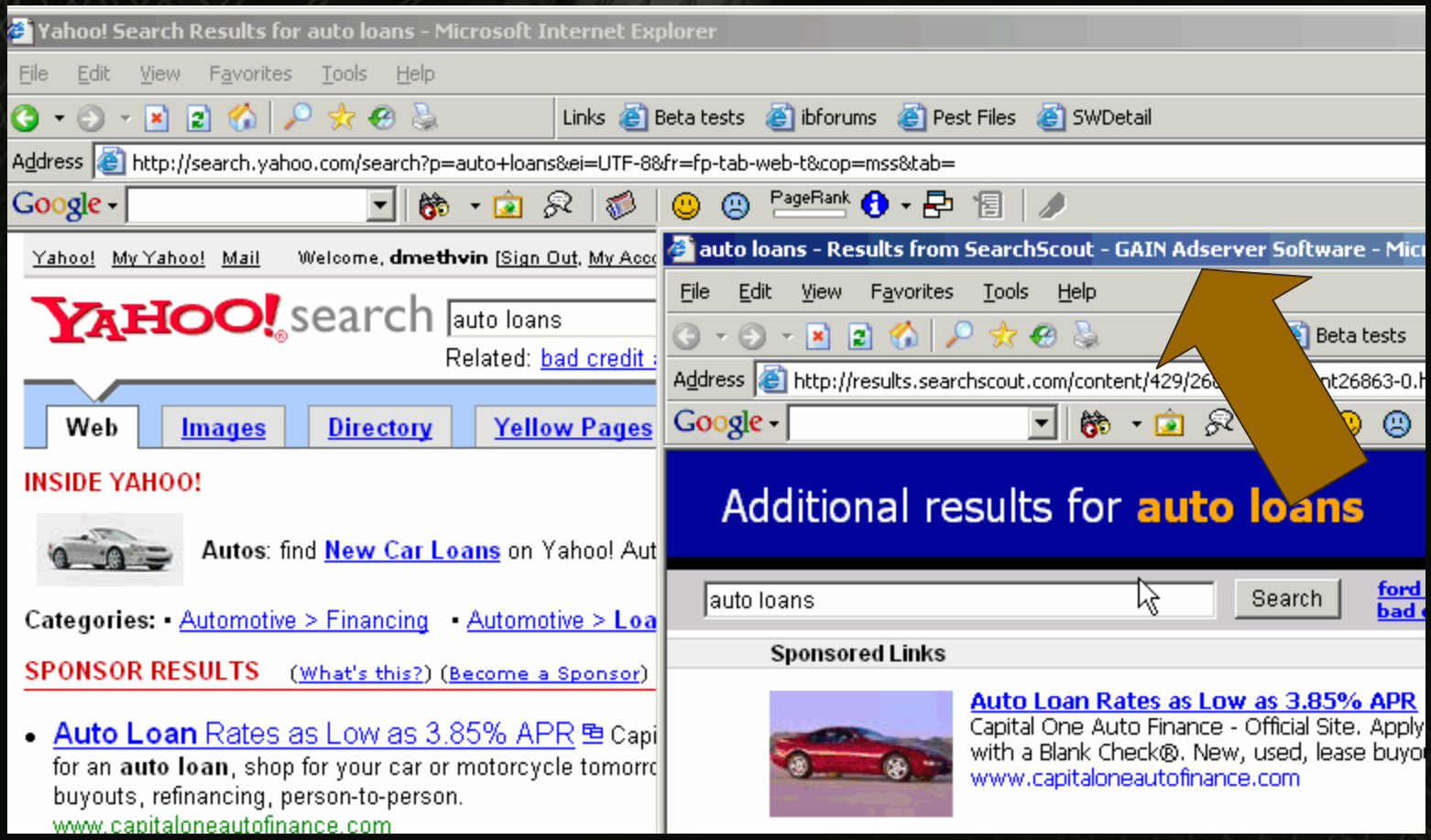
- Una chance da non perdere

  In questo caso, oltre alla pubblicità, otteniamo visite al sito web e altre pagewiews per qualunque banner nel NOSTRO network.

- Siti affetti

  Tra gli altri ricordiamo: MSN, Yahoo, Amazon, Kmart, Google, Lycos, Altavista, A9, CNN, The New York Times, Visa, Mastercard, American Express, Berkley, CBS, NBC, Microsoft, Adobe, Barnes&Nobles, IBS, Citybank, BankOfAmerica


Delta Air Lines - Find airline tickets, manage your SkyMiles account, or chec
Brought to you by the Zango Search Assistant - Microsoft Internet Exp
File Edit View Favorites
Back
Search
Favorites
Address
http://www.hawaiianair.
Hawaii Starts Here: Hawaiian Airlines is yo
e Hawaiian Islands
ervations
Flight Schedule/Info
HAWAIIAN AIRLINES.
Plan Your Trip
Hotel & Car
Vacation Packages
Activities, Tours & D
Make Flight Reservation
Book with Coupons
Book an E-Award
View My Reservations
Vacation Packages
Air , Hotel and Car
Book a Package
Web Check-In
Hele On
Earn 1,000 Bonus Miles*
Web Check-In
Demo | FAQ
*1st Web Check-In Only. Ends 6/30/2004
Flight Schedule | Flight Tracking | Route Map | Destination Info
Sign Up to receive special fares & offers from Hawaiian Airlines
Special Offers - Li
Each way Starting at $139* USD
Each way Starting at $
Start
Untitled - Windows Medi...
Delta Air Lines - Find airli...


Yahoo! Search Results for auto loans - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links Beta tests ibforums Pest Files SWDetail
Address http://search.yahoo.com/search?p=auto+loans&ei=UTF-8&fr=fp-tab-web-t&cop=mss&tab=
Google PageRank
Yahoo! My Yahoo! Mail Welcome, dmethvin [Sign Out, My Acc
YAHOO! search auto loans
Related: bad credit
Web Images Directory Yellow Pages
INSIDE YAHOO!
Autos: find New Car Loans on Yahoo! Aut
Categories: • Automotive > Financing • Automotive > Loa
SPONSOR RESULTS (What's this?) (Become a Sponsor)
• Auto Loan Rates as Low as 3.85% APR Capi
for an auto loan, shop for your car or motorcycle tomorro
buyouts, refinancing, person-to-person.
www.capitaloneautofinance.com
auto loans - Results from SearchScout - GAIN Adserver Software - Mic
File Edit View Favorites Tools Help
Beta tests
Address http://results.searchscout.com/content/429/26
nt26863-0.H
Google
Additional results for auto loans
auto loans
Search
ford
bad
Sponsored Links
Auto Loan Rates as Low as 3.85% APR
Capital One Auto Finance - Official Site. Apply
with a Blank Check®. New, used, lease buyo
www.capitaloneautofinance.com

Mascheramento e sostituzione

Raccolta dati Mkt

- Una base dati enorme

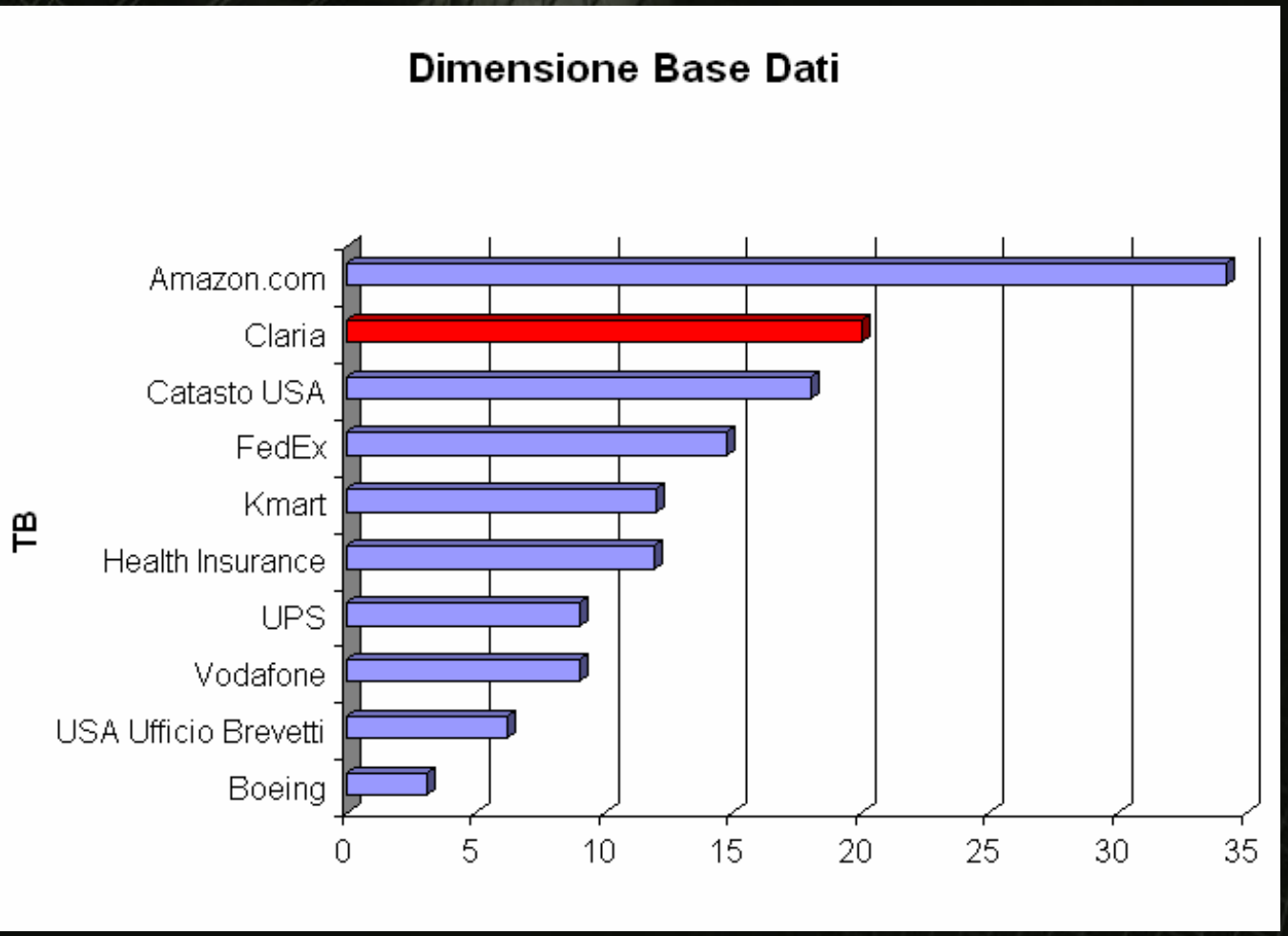
  Contenente abitudini di navigazione, siti visitati, banner visti, acquisiti effettuati

- Informazioni in vendita

  Sono disponibili statistiche generali o statistiche dettagliate sul proprio settore di attività

- Marketing mirato

  La disponibilità di storico consente di effettuare manovre di Marketing con target estremamente preciso (es: *"tutti gli utenti che hanno comprato da Amazon e visitato almeno una volta RyanAir"*).


Dimensione Base Dati
TB
Amazon.com
Claria
Catasto USA
FedEx
Kmart
Health Insurance
UPS
Vodafone
USA Ufficio Brevetti
Boeing
0
5
10
15
20
25
30
35

Commission theft

- Il referral come mercato

  Il mercato delle commissioni per referente è affermato e conta una movimentazione di denaro oltre $. 850.000.000,00

- Commissioni dignitose

  Le commissioni per la vendita variano dal 3% al 15% a seconda del network e sono erogate in modo totalmente automatico.

- La vita dei piccoli

  Per molti siti di informazione o riviste online il pagamento delle commissioni rappresenta la prima fonte di reddito ed a volte anche l'unica possibile.


Venditore
Sito Affiliato

Commission theft

- Interposizione

  Mediante l'apertura di nuove finestre e/o parti nascoste di codice nella pagine lo Spyware (Gator/180search/WhenU) si interpone nella transazione

- Furto di commissioni

  Le commissioni "legittime" vengono quindi traghettate alla società dello spyware e sottratte al legittimo proprietario.


Venditore
Sito Affiliato
CLARIA
Gator eWallet

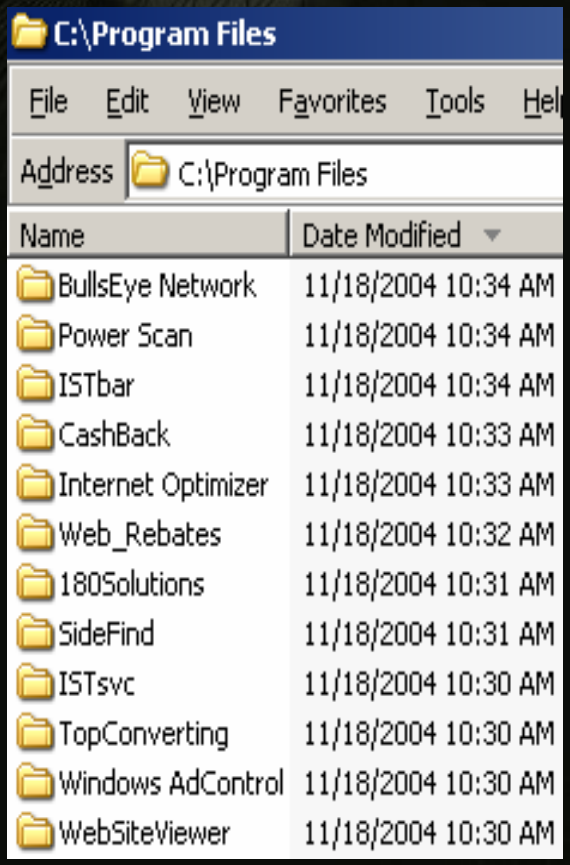
Commission theft

> Lauti guadagni

Nel mese di Marzo 2003, Gator ha incassato per la sottrazione di commissioni a MSNBC sul solo cliente Dell $100.000,00

Installazioni non autorizzate

- Incentivazione a delinquere
  - Gator Corp, Claria e 180search promuovono la installazione del software da parte di "terze parti"
- Commission per Install
  - Per ogni installazione dello spyware sulla macchina viene riconosciuta una commissione al sito installatore di circa $.0,70.
  - Un worm che infetti 20.000 macchine avrà quindi un ritorno economico di circa $.14.000,00
- Vantaggi per entrambi
  - Con questo meccanismo noti Hacker ottengono lauti guadagni mentre la società di spyware è tutelata da eventuali lamentele poiché "non colpevole" di azioni compiute in altri stati e altre giurisdizioni.
- Veri e propri worm
  - I software utilizzati installano spyware "a cascata" per ottimizzare le revenues.


C:\Program Files
File Edit View Favorites Tools Hel
Address C:\Program Files
Name Date Modified
BullsEye Network 11/18/2004 10:34 AM
Power Scan 11/18/2004 10:34 AM
ISTbar 11/18/2004 10:34 AM
CashBack 11/18/2004 10:33 AM
Internet Optimizer 11/18/2004 10:33 AM
Web_Rebates 11/18/2004 10:32 AM
180Solutions 11/18/2004 10:31 AM
SideFind 11/18/2004 10:31 AM
ISTsvc 11/18/2004 10:30 AM
TopConverting 11/18/2004 10:30 AM
Windows AdControl 11/18/2004 10:30 AM
WebSiteViewer 11/18/2004 10:30 AM


Dietro allo Spyware
Venture Capitals e Market Share

Non pirati, ma capitali

- Enormi Venture Capitals

  I top players del mercato dello spyware non fanno capo ad organizzazioni mafiose e/o residenti in paradisi fiscali, ma a enormi venture capitals quotate

- Capitale di rischio

  Se è pur vero che sono "capitali a rischio" è anche vero che NESSUNA di queste aziende ha chiuso con meno di un incremento netto di fatturato del 7% per ogni mese dei trascorsi 2 anni.

Composizioni Societarie

- 180 Solutions (Zango, ncase)
  - Specrtum Equity Investors: $40.000.000
  - *(che investe in Cellular One, Loews CinePlex, EutelSat, MetricsDirect)*
- Claria (Gator, GAIN)
  - Investimenti totali: $.58.000.000
  - US Venture partners
  - *(che investe anche in Cisco, Iomega, Sun, AskJeeves, Cogency, Epic, Sun, Sundisk, Alcatel)*
  - GrayClock
  - *(che investe anche in Redhat DoubleClick, LinkedIn, Lumigent, Raptor, SightPath)*
  - CrossLink Capital
  - *(che investe anche in EMachines, Cirrus, Borderbund, TiVb)*

Composizioni Societarie

- Claria (Gator, GAIN)
  - Garage Technology Ventures
    (che investe anche in Psionic, Tripwire, The Motley Fool)
  - Rosewood Stone Group
    (che investe anche in Allaire, Concentric, Excite!, Prospero, Salon.com, Redhat DoubleClick, LinkedIn, Lumigent, Raptor, SightPath)
  - Investor AB
    (che investe anche in Ericsson, Saab, ABB, Atlac Copco, Electrolux, Scania)
  - Technology Corossover Venture
    (che investe anche in BrightMail, C|Net, eBags, Expedia, eHarmony, NetFix, Real)

Composizioni Societarie

- DirectRevenue (Optimixer)
  - Insight Venture: $.20.000.000
  - Technology investment Capital Group: $6.700.000
- eXact Advertising (BergainByddy)
  - Technology investment Capital Group: $15.000.000

Principali Clienti

- Utenti di Gator

  ING Direct, Apple Store, Avon, Crysler, Disneyland Resort, Expedia, Palm, Priceline, uBid, Verizon, Western Union, Rail Europe, Sun Microsystems

- Utenti whenU

  Travelocity, EBay, Priceline, Thrifty, Best Western, Time Life Walt Disney Classics, KaBloom, Virgin Mobile, Sprint PCS, T-Mobile, Verizon, Chase, ING Direct, AmericanExpress,Ameriquest, the University of Phoenix Online, Lloyds TBS,

Caccia allo Spyware

Principali software

Principali Anti-Spyware

> Spybot Search&Destroy

Freeware - http://security.kolla.de

Principali Anti-Spyware

> Ad-Aware

Freeware/Shareware - http://www.lavasoftusa.com

Principali Anti-Spyware

> Microsoft Anti-Spyware Beta

Freeware - www.microsoft.com/athome/security/spyware/software/default.mspx

Matteo G.P. Flora

http://www.lastknight.com
lk@lastknight.com